Spear Phishers: Angling to Steal Your Financial Info

Customers of a telecommunications firm received an e-mail recently explaining a problem with their latest order. They were asked to go to the company website, via a link in the e-mail, to provide personal information—like their birthdates and Social Security numbers. But both the e-mail and the website were bogus.

It's a real-life, classic case of "phishing"—a virtual trap set by cyber thieves that uses official-looking e-mails to lure you to fake websites and trick you into revealing your personal information.

It's also an example of an even more mischievous type of phishing known as "spear phishing"—a rising cyber threat that you need to know about.
Instead of casting out thousands of e-mails randomly hoping a few victims will bite, spear phishers target select groups of people with something in common—they work at the same company, bank at the same financial institution, attend the same college, order merchandise from the same website, etc. The e-mails are ostensibly sent from organizations or individuals the potential victims would normally get e-mails from, making them even more deceptive.

How spear phishing works. First, criminals need *some* inside information on their targets to convince them the e-mails are legitimate. They often obtain it by hacking into an organization's computer network (which is what happened in the above case) or sometimes by combing through other websites, blogs, and social networking sites. Then, they send e-mails that look like the real thing to targeted victims, offering all sorts of urgent and legitimate-sounding explanations as to why they need your personal data. Finally, the victims are asked to click on a link inside the e-mail that takes them to a phony but realistic-looking website, where they are asked to provide passwords, account numbers, user IDs, access codes, PINs, etc.

Criminal gain, your loss. Once criminals have your personal data, they can access your bank account, use your credit cards, and create a whole new identity using your information. Spear phishing can also trick you into downloading malicious codes or malware after you click on a link embedded in the e-mail…an especially useful tool in crimes like economic espionage where sensitive internal communications can be accessed and trade secrets stolen. Malware can also hijack your computer, and hijacked computers can be organized into enormous networks that can be used for denial of service attacks.

How to avoid becoming a spear phishing victim. Law enforcement takes this kind of crime seriously. The FBI along with their partners including the U.S. Secret Service and investigative agencies within the Department of Defense work cyber investigations. What can you do to make sure you don't end up a victim in one of our cases?

- Keep in mind that most companies, banks, agencies, etc., don't request personal information via e-mail. If in doubt, give them a call (but don't use the phone number contained in the e-mail—that's usually phony as well).
- Use a phishing filter…many of the latest web browsers have them built in or offer them as plug-ins.

Source: U.S. Department of Justice.